SECTION C - PERFORMANCE WORK STATEMENT

C.1 BACKGROUND

The Army National Guard (ARNG) Personnel (G1) is responsible for creating, managing, and executing all manpower and personnel plans, programs, and policies across all the ARNG Directorates. The Reserve Component Manpower System-Guard (RCMS-G) and the SMMS are used to support and enhance the ARNG G1 decision-making process. Most data input to this system are raw data that indicate the status of Reserve Component personnel and the changes that have occurred to the force during the current reporting period. SMMS/RCMS-G processes these data and converts them into useful information for the users. The output generated may take on many forms, such as graphical output showing grade and year-of-service profiles, a budget book showing the cost of the manpower program over the Future Years Defense Programs (FYDP), or statistics showing personnel readiness during mobilization. SMMS/RCMS-G provides its users with the ability to readily access the personnel data, extract and integrate the data from multiple sources, refine and improve the data, and make it available to decision makers in a form that makes trends and key issues apparent for making critical Guard-wide decisions.

SMMS/RCMS-G aggregates data from multiple sources enabling users to view, manipulate, and analyze manpower-related information. Its features and capabilities have grown over the years in sophistication and quantity. SMMS/RCMS-G is supported by a large number of hardware and software systems that include over 150 different modules, applications, and data sources. SMMS/RCMS-G leverages the Microsoft technology stack and other technologies. It exposes a graphical user interfaces and supports a large number of concurrent users across many functional and operational areas. SMMS/RCMS-G features a robust enterprise data warehouse which aggregates sources of information from many disparate systems. It provides data to and receives data from a multitude of other systems, such as Reserve Component Automation Systems (RCAS), Army Training Requirements and Resources System (ATRRS), Standard Installation and Division Personnel Reporting System (SIDPERS), Total Army Personnel Database-Guard (TAPDB-G), Medical Protection System (MEDPROS), Contact Pre-Qualification Processing System (CPPS), and many others.

C.1.1 PURPOSE

The purpose of this requirement is to provide services for the SMMS and Reserve Component Management System-Guard (RCMS-G). The RCMS-G was identified as an aging system by the Army TBAI office, and a target sunset date is set for 2022. The ARNG G1 agreed to sunset RCMS-G in time and migrate enduring RCMS-G capabilities into the SMMS. SMMS/RCMS-G is entering into the Business Capability Acquisition Cycle process in order to do the following:

1) Formulate the Problem Set;
2) Garner additional resources and support from ARNG Headquarters and Department of the Army (HQDA); and
3) Develop the Plan of Action and Milestones to Sunset RCMS-G by 2022.

C.1.2 AGENCY MISSION

To support the ARNG G1 mission, the SMMS/RCMS-G suite of applications and modules were developed to provide ARNG action officers and senior leaders with critical manpower information needed to enhance their decision-making process. SMMS/RCMS-G aggregates data from multiple authoritative data sources and presents results in the form of user information, such as reports, dashboards, or data files, which are delivered to authorized locations, or presented via Web portal.

C.2 SCOPE

The SMMS/RCMS-G suite is used to access, gather, and present manpower readiness data to ARNG decision makers. This requirement includes the operations, maintenance, data operations, and analytical support for the SMMS/RCMS-G system and its users as well as making changes to the system to ensure compatibility with evolving technologies. In the performance of this contract, ARNG expects the contractor to provide innovative solutions that bring technical and operational improvements to the ARNG and its SMMS/RCMS-G users and customers. In providing services to SMMS/RCMS-G, the contractor shall coordinate its efforts with a number of other contractors and government organizations and maintain agreements with those organizational entities.

The scope of this contract includes the following:

1. Maintaining the operational readiness of the SMMS/RCMS-G applications, modules, and interfaces;

2. Maintaining the operating system (OS) of the SMMS servers in the Primary environment and associated Continuity of Operations Plan (COOP) environment;

3. Supporting data operations by providing ongoing management of data feeds, maintenance of SMMS/RCMS-G metrics, and the processing of production data;

4. Providing changes to SMMS/RCMS-G analytical functions;

5. Providing project management and execution of all changes to the SMMS/RCMS-G applications, modules and interfaces, including the integration of selected ARNG G1 systems into the SMMS/RCMS-G environments;

6. Producing, updating, and maintaining the Business Process Reengineering (BPR), Department of Defense (DoD) Architecture Framework (DoDAF), and Business Enterprise Architecture (BEA) documents for all changes to the SMMS/RCMS-G suite;

7. Identifying and eliminating vulnerabilities to SMMS/RCMS-G and;

8. Achieving and maintaining information assurance and accreditation of the SMMS/RCMS-G and SMMS systems in accordance with (IAW) DoD and federal standards (to include the Contact Pre-Qualification Processing System [CPPS], which supports lead generation from 1-800-GO-GUARD.COM). CPPS is administered by another source, IO Studios, but is included within the SMMS/RCMS-G accreditation boundary. The contractor shall purchase software licenses in order to fulfill the requirements of this solicitation. Software must be procured through the Army's Computer Hardware and Enterprise Services and Support (CHESS) contract, or other appropriate source. The TPOC must approve all purchases and sources in writing.

C.3 CURRENT ENVIRONMENT

The current environment is outlined in Section J, Attachment B.

C.4 OBJECTIVE

The overall objective of this requirement is to sunset RCMS-G and migrate enduring RCMS-G capabilities into the SMMS by 2022.

C.5 TASKS

C.5.1 TASK 1 – PROJECT MANAGEMENT

The contractor shall provide project management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS).

C.5.1.1 COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include contractor key personnel, representatives from the directorates, other relevant Government personnel, and the CO, CS, COR, and TPOC.

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting agenda for review and approval by the CO prior to finalization. The agenda shall include at a minimum the following topics/deliverables:

a. Points of Contact (POC) for all parties;

b. Personnel discussion (i.e., roles and responsibilities and lines of communication between the contractor and Government);

c. Staffing plan status;

d. Transition-In Plan and discussion;

e. Security discussion and requirements, i.e., building access, badges, Common Access Cards (CACs);

f. Invoicing requirements; and

g. Final Baseline Quality Control Plan (QCP).

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present at the meeting. The contractor shall draft and provide a Kick-Off Meeting Minutes Report documenting the Kick-Off Meeting discussion and any action items.

C.5.1.2 PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide a MSR. The MSR shall include the following:

a. Activities during the reporting period by tasks (including, ongoing activities, new activities, activities completed, and progress to date on all activities). Each section shall start with a brief description of the task.

b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.

c. Notification/information about any revoked or expired contractor personnel security clearances.

d. Government actions required.

e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).

f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).

g. Accumulated invoiced cost for each CLIN up to the previous month.

h. Projected cost of each CLIN for the current month.

C.5.1.3 CONVENE TECHNICAL STATUS MEETINGS

The contractor Project Manager (PM) shall convene a monthly Technical Status Meeting with the CO, CS, COR, TPOC, and any other necessary Government stakeholders (Section F, Deliverable 05). The purpose of the meetings is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items to the CO, CS, COR, and TPOC.

C.5.1.4 PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a draft PMP for TPOC/COR review. The final PMP shall incorporate TPOC/COR comments approved by the COR.

The PMP shall:

a. Describe the proposed management approach;

b. Contain detailed Standard Operating Procedures (SOPs) for all tasks;

c. Include milestones, tasks, and subtasks required in this TO;

d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations;

e. Describe in detail the contractor’s approach to risk management under this TO including the transition in;

f. Describe in detail the contractor’s approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government; and

g. Include the contractor’s Baseline QCP.

C.5.1.5 UPDATE THE PROJECT MANAGEMENT PLAN

The PMP is an evolutionary document that shall be updated annually at a minimum. The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.6 TRAVEL REQUEST AND PREPARE TRIP REPORTS

The contractor shall submit a Travel Request (TR) for each individual participant. All TRs shall at a minimum include the information below in this section required for Trip Report. All TRs shall be reviewed and approved by the TPOC prior to participant travel.

The contractor shall submit Trip Reports to the TPOC, no later than (NLT) five business days after completion of a trip for all long distance travel. Long distance travel is defined as travel over 50 miles from Washington, DC. Local travel will not be reimbursed.

The Trip Report shall include the following information:

a. Name(s) and title(s) of personnel who traveled;

b. Dates of travel;

c. Destination(s);

d. Purpose of trip;

e. Cost of the trip;

f. Approval authority; and

g. Summary of events.

The contractor shall keep a summary of all long-distance travel, including but not limited to the name of the employee, location of travel, duration of trip, and Point of Contact (POC) at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained.

C.5.1.7 PROVIDE QUALITY CONTROL MANAGEMENT

The contractor shall develop and maintain an effective QCP to ensure services are performed in accordance with Section C. The contractor’s QCP is the means by which it assures that the services performed complies with the requirements of the resulting task order. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services.

The contractor’s QCP shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The QCP shall describe how the appropriate methodology integrates with the Government's requirements.

The QCP shall include the following:

1. Organization and resources. Organization chart and communication interfaces for all personnel performing Quality Control (QC) functions. Identification of the authority of the QCP manager to monitor and control functions, and to implement remedial and preventive actions;

2. Specific inspection techniques and methods tailored to each functional area; and

3. Procedures for corrective action.

The contractor shall update the QCP submitted with its proposal and then provide a final baseline QCP as required in. The contractor shall periodically update the QCP as required as changes in program processes are identified.

C.5.1.8 QUALITY CONTROL RESPONSIBILITIES

The contractor's quality control team shall monitor and promote adherence to established SMMS/RCMS-G service levels by analyzing Performance Requirements Summary (PRS), performance data, as well as existing policies and procedures.

The contractor's quality control team shall:

1. Formulate and enforce internal work quality standards;

2. Ensure all users are notified with service request ticket status;

3. Produce and provide performance reports;

4. Conduct periodic performance reviews to improve current operations;

5. Maintain statistical data in order to demonstrate performance trends;

6. Maintain summary performance data throughout the life of the Contract;

7. Conduct independent quality assurance reviews of closed tickets to ensure they are managed properly;

8. Ensure service request tickets are closed;

9. Prepare training plans for the development of the staff and to improve service support;

10. Identify user training needs based on analysis of tickets;

11. Investigate all report statistics and analysis as appropriate;

12. Investigate missed requirements and identify root causes for the non-compliance; and

13. Identify issues (technical, management, or otherwise) that prevent the contractor from meeting the Service Level Agreements (SLAs) and/or other operational goals.

C.5.1.9 OPSEC SOP/PLAN

The contractor shall develop an Operational Security (OPSEC) Standard Operating Procedure (SOP)/Plan and provide it to the TPOC/COR within 90 calendar days of contract award to be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This SOP/Plan shall include a process to identify the government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. The contractor shall implement OPSEC measures as required by the Government. In addition, the contractor shall identify an individual who will be an OPSEC coordinator. The contractor shall ensure this individual becomes OPSEC Level II certified within 90 days of appointment as OPSEC coordinator in accordance with AR 530-1. Contractor shall provide a copy of the certification to the COR and TPOC NLT 15 days after completion.

C.5.2 TASK 2 – TRANSITION-IN

The contractor shall update the draft Transition-In Plan provided with its proposal and provide a final Transition-In Plan as required in Section F. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. All transition activities shall be completed within 45 to 90 calendar days after approval of final Transition-In Plan.

Transition-in shall require coordination with the incumbent contractor for acceptance of the project. The contractor shall perform a joint inventory of all Government-furnished equipment (GFE) with the incumbent contractor and the TPOC or Property Book Officer. All discrepancies and problems shall be noted and submitted to the CO, CS, COR, and TPOC for resolution. The contractor shall inventory all GFE listed on DA Form 3161. The contractor shall have its key personnel available at the project start date. At the beginning of phase-in, the contractor shall also certify to the CO, CS, COR and TPOC, that all of the contractor’s employees meet the training criteria as specified in Sections H.2.2 through H.2.5.

The key transition objectives for the transition of the SMMS/RCMS-G services to the TO awardee during the transition-in period are to:

1. Minimize transition impact to the user community;
2. Ensure no breaks in service availability;
3. Maintain existing service quality and performance levels;
4. Ensure a transparent and seamless transition; and
5. Ensure that the IT security posture during transition is maintained at current levels without creating gaps and/or vulnerabilities.

The contractor shall execute the Incoming Transition Plan in a manner that positions the contractor to successfully assume responsibility for maintaining operational readiness of the SMMS/RCMS-G systems. At a minimum, SMMS/RCMS-G support includes:

1. Standing up the facility that meet the requirements presented in the PWS;
2. Hiring, training and obtaining security clearance and certifications for all staff;
3. Transferring all knowledge required to operate and maintain the environment and to provide user support through the SD; and
4. Establishing operational relationships with other organizations involved in the operations.

The contractor shall manage and perform all tasks required to transition operational support from the incumbent contractor.

The incoming contractor must understand that the incumbent's primary responsibility is to maintain operational capabilities of the SMMS/RCMS-G Suite during the transition period.

Therefore, the contractor shall not assume the incumbent staff will be available to provide dedicated or extensive assistance. It is the responsibility of the contractor to: obtain access to the operational systems, review existing materials to gain an understanding of the current operations and present a comprehensive plan for moving equipment, if needed, in a manner that minimizes disruption to ongoing operations. The contractor shall work with the TPOC to obtain this information. The TPOC will not dictate the approach, but must approve all plans.

The contractor shall understand that the SMMS/RCMS-G systems and applications along with their interfaces have been custom developed over many years. The ARNG has SOP and other system documentation to be provided to the contractor prior to Kick-Off meeting.

C.5.2.1 REQUIRED TASKS FOR TRANSITION

Facility: The contractor shall establish the operational and support facility, which will house all efforts associated with the technical requirements in this PWS. The proposed facility must meet the minimum requirements. See Section H.

C.5.2.2 KNOWLEDGE AND EQUIPMENT TRANSFER

The contractor shall:

1. Develop and execute a Transition-In Plan;
2. Conduct an inventory of GFE and IT assets;
3. Establish management processes and controls and other tasks necessary to support the transition process;
4. Inventory and verify all software titles and license keys settings necessary to operate and maintain the SMMS/RCMS-G systems and environments;

5. Inventory all source code, stored procedures, development and administrative tools, configuration settings, etc. necessary to operate and maintain the SMMS/RCMS-G systems and environments;

6. Gain access to and establish an understanding of all Enterprise Mission Assurance Support Service (eMASS) and the various controls, inherited controls, and associated artifacts;

7. Assume responsibility for moving GFE equipment from the current SMMS/RCMS-G service provider's to the contractor's facility; and

8. Clean up the ticket data and transition tickets to the new ticketing system.

C.5.2.3 SPECIFIC TRANSITION-IN REQUIREMENTS:

The contractor shall develop and execute a Transition-In Plan that includes at a minimum:

1. Specific tasks to be performed and the resources assigned to them;

2. Task dependencies and relationships;

3. Proposed task duration; and

4. Major milestones.

The transition schedule shall be documented within the Incoming Transition Plan. At a minimum, the set of tasks shall include:

1. Personnel actions;

2. Hiring, obtaining/verifying clearance and certifications;

3. Accounts – requesting appropriate accounts from the Government;

4. Training (including any required certifications);

5. Schedule shall include milestones for percentage of staff ready for operations and maintenance (O&M) duties;

6. Facility. This section shall address progress towards outfitting the contractor's facility including subcontracts, leases, environmental issues, safety and security, etc. in the implementation of their transition strategy;

7. ARNG domain knowledge transfer;

8. Readiness reviews demonstrating the capability to operate and maintain the systems and environments.

The contractor shall schedule and conduct weekly status meetings to report and review progress of the transition (Section F, Deliverable 16)

Within the transition-in period and prior to formally taking over operational responsibilities, the contractor shall demonstrate readiness to proceed. The ARNG will review the level to which the contractor was able to accomplish the transitional tasks. The contractor shall complete the following within the transition period in order to proceed with the task order:

1. The contractor shall demonstrate ability to take over administrative management of all SMMS/RCMS-G elements outlined in this PWS.

2. Demonstrate operational readiness of the contractor’s facility, including:

    a) Completely outfitted physical office space for the all of the contractor’s personnel;
    b) Temporary office and meeting space for the ARNG personnel;
    c) Service Desk space;
    d) Telephone system supporting the Service Desk in a manner that supports SLAs outlined in this solicitation;
    e) Physical access security; and
    f) Connectivity to SMMS/RCMS-G and associated networks and environments.

3. Demonstrate functionality of the ticketing system.

4. Demonstrate that the contractor staff has the certifications required to operate the ARNG’s system management elements as outlined in this PWS.

5. Demonstrate that the contractor’s staff understands established ARNG policies and procedures. See Attachment R for applicable DoD and Army directives, instructions and regulations.

6. Secure all user privileges and access needed to conduct O&M to support this solicitation.

7. Demonstrate successful execution of daily, weekly, and monthly processing activities as needed to fulfill the O&M needs of this solicitation.

8. Successfully support 45 days of data processing during transition period to include a minimum of two End of Month (EOM) processing periods.

C.5.3 TASK 3 – ENTERPRISE CONTRACTOR MANPOWER REPORTING APPLICATION (ECMRA)

The contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site and provide to the CO, CS, COR and TPOC via email with a copy of the report and notification/confirmation of submission to the site. The secure data collection site is operated and maintained by the Office of the Assistant Secretary of the Army-Manpower & Reserve Affairs (ASA-M&RA). This task does not change the contract type basis.

Accounting for contractor Support: The contractor shall completely fill in all required data fields using the following web address: http://www.ecmra.mil/. Reporting inputs shall be for the labor executed during the period of performance during each Government fiscal year (FY), which runs from October 1 through September 30. Inputs shall be reported annually and are due NLT October 31 of each calendar year, beginning with 2019, (Section F, Deliverable 17). Contractors may direct questions to the help desk at http://www.ecmra.mil.

C.5.4 TASK 4 – SMMS AND RCMS-G SYSTEMS OPERATIONS AND MAINTENANCE

C.5.4.1 SMMS OPERATIONS AND MAINTENANCE

SMMS is transitioning from Acquisition Logistics and Technology Enterprise System (ALTESS) Infrastructure as a Service (IaaS) Data Center to the Microsoft Azure Cloud environment.

The contractor shall operate SMMS at the designated host facilities in accordance with the IaaS table shown in Figure 1 (Section J, Attachment F). The ALTESS Data Center provides IaaS styled hosting environment for the physical infrastructure (racks, power, Local Area Network (LAN)/Wide Area Network (WAN), servers, firewalls, security devices, and other common services) and manages Virtual Machine (VM) servers hosting the SMMS module.

The contractor shall prepare and execute a plan to migrate to the Azure Development, Testing, and Production environments.

The contractor shall adopt and maintain administrative, technical, and physical safeguards and controls that are required for the security level and services being provided, in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time of contract award) found at: http://iase.disa.mil/cloud_security/Pages/index.aspx . Note: The new cyber incident reporting requirements of SRG section 6.4 become enforceable by the Government upon the effective date of the information collection governing the new reporting requirements (see DFARS case 2013-D018). However, this does not abrogate, limit, or otherwise affect the contractor's obligation to comply with any other cyber incident reporting or other reporting requirement that is contained in this solicitation.

The contractor shall perform maintenance necessary to respond to any Advisory, Conciliation and Arbitration Service (ACAS) scans ran by host facilities.

The contractor shall comply with all Army Information Assurance Vulnerability Alerts (IAVAs) in regards to upgrades and scheduling of upgrades.

The contractor will coordinate with ALTESS and/or AZURE to schedule Full and Differential backups of VMDK files. ALTESS will do file level backups/restores on all VMs including VM snapshots.

The contractor shall utilize ALTESS and/or AZURE provided Structured Query Language (SQL) 2014 and MySQL NetBackup agents to back up and restore Database Servers.

The contractor must manage Development, Test, Staging, and Production environments to ensure code is promotable to production with consistent results.

The contractor shall maintain the SMMS virtual machines at both the hosted environment and the COOP environment to ensure operational capability and security compliance.

The contractor Admins will have access to the ALTESS servers via a Citrix/Management server and have full administrative OS rights on all Enclave Virtual Machines (VM). Contractor admins will not have access to the VMware hypervisors.

The contractor is responsible for all network setup beyond ALTESS TLA stack.

The contractor shall be responsible for the management of the OS, Application layer and all SMMS Web Sites.

In the event of a situation that impacts system availability, the contractor shall notify the TPOC as soon as possible after detection of the issue but not more than 12 hours after detection.

C.5.4.2 RCMS-G OPERATION AND MAINTENANCE

RCMS-G is hosted in the ARNG Temple Jr. Army National Guard Readiness Center (TARC) in the Installation Processing Node (IPN) located in Arlington, VA.

RCMS-G must be subsumed and/or integrated into SMMS no later than September 30, 2021.

The TARC IPN provides (IaaS) support and maintains a virtualized hosting environment for the system, ensuring that the virtual infrastructure is available to the maximum extent possible. The contractor will be granted vCenter console access to view all VMware performance counters for their servers and have the ability to attach to the server console, reboot, shutdown, and turn off ARNG-HRM servers.

The contractor shall maintain the SMMS/RCMS-G VMs at ARNG TARC IPN through a pro Active coordination with ARNG-G6 -- staff responsible for signal/computer management.

The contractor shall perform routine service and maintenance on a scheduled basis. Emergency maintenance for system operations will require support on a 24/7 basis.

The contractor shall mitigate findings uploaded to the Vulnerability Management System (VMS), ensuring that all systems remain fully patched and are Army Information Assurance Vulnerability Alert (IAVA) compliant.

The contractor shall ensure that all systems remain full DISA Standard Technical Implementation Guide (STIG) compliant. The contractor shall document in VMS or with a Memorandum for Record any STIG finding that cannot be mitigated stating why the finding cannot be applied and any mitigation in place to limit the vulnerability created by the STIG non-compliance.

Due to the need to comply with higher guidance from Network Enterprise Technology Command (NETCOM) and US Cyber Command the following permissions and clients will remain in effect for the system.

Domain Administrators and IMO IA personnel will remain in the local administrators groups on the servers. All personnel with access will maintain current training (IA, PII, HIPAA, etc.) prior to being granted access.

The contractor shall ensure Army Host Based Security System (HBSS), System Center Configuration Manager (SCCM), and Antivirus clients are installed and functional.

The contractor is responsible for backing up RCMS-G systems and databases to the IMO provided backup Common Internet File System (CIFS) share using either the Microsoft provided tools, or third party tools provided by the Government.

The contractor shall ensure backups are not encrypted or compressed in order to maximize the efficiencies gained by using the provided backup hardware.

The contractor shall monitor storage utilization and identify requirements for additional storage at least 2 weeks in advance.

The contractor shall coordinate with ARNG G6 and NETCOM to provide the required web proxy and filtering.

The contractor shall be responsible for ensuring annual Federal Information Security Management Act (FISMA) requirements are met. These requirements include annual system security assessment, annual test of security controls, and annual testing of the system's contingency plan.

The contractor shall operate RCMS-G at the ARNG IPN hosting facility in accordance with the IaaS table shown as Figure 1 (Section J, Attachment F). RCMS-G consists of production elements (ARNG G1 data store databases, RCMS-G modules and Web server) The ARNG TARC IPN provides IaaS styled hosting environment for the physical infrastructure (racks, power, Local Area Network (LAN)/Wide Area Network (WAN), servers, firewalls, security devices, etc.) as well as for the OS of the servers hosting the RCMS-G modules.

The contractor shall maintain the RCMS-G test system hosted at the ARNG TARC IPN to be consistent with the production environment.

The contractor shall prepare plans and execute the transition and/or integrate capabilities and data to other systems as directed by the Government while maintaining capabilities with minimal impact to users.

The contractor shall maintain the RCMS-G virtual machines at ARNG IPN and ARNG COOP environment through a pro-active coordination with ARNG-G6 to ensure operational capability and security compliance.

In the event of a situation that impacts system availability, the contractor shall notify the TPOC as soon as possible after detection of the issue but not more than 12 hours after detection.

C.5.4.3 DATABASE(S) MAINTENANCE

The contractor shall manage the performance and availability of these SMMS/RCMS-G databases that comprise the SMMS/RCMS-G Suite data store. As of April 2018 the environment is comprised of Microsoft SQL 2012 and 2014. The contractor shall migrate any existing servers to the latest approved Microsoft SQL server database release.

The structure and size of the SMMS databases are the following:

- SMMSDB01 : 63 databases, 12,086 tables with 1.2TB
- SMMSDB02 : 65 databases, 33,295 tables with 1.5TB
- SMMSDB03 : 33 databases, 1,098 tables with 0.7TB

The structure and size of the RCMS-G databases are the following:

- RCMSDB01: 68 databases, 9,046 tables with 1.2TB
- RCMSDB02: 83 databases, 21,000 tables with 1.5TB
- RCMSDB03: 26 databases, 31,434 tables with 2.9TB

The structure and size of SMMS is comprised of the VMs listed in Attachment X at the ALTESS Data Center.

The AZURE environment shall include Development, Test/Staging, and Production environments and may be expanded or decreased as necessary to meet SMMS/RCMS-G mission requirements.

The contractor shall Monitor and resolve performance issues, data access and setup, monitor status of scheduled backups, coordinate and write processes for inbound and outbound data transfers, and create, schedule to run and monitor all required ETL (Extracting, Transforming and Loading) processes.

The contractor shall be responsible for:

Developing and maintaining replication processes to ensure accurate and available data in the various production environments;

Providing ongoing coordination with software maintenance team(s) for tailored products, modules, and models database and best practices support;

Assessing and improving the database performance, mod schema, manage indexes, produce roll up tables and views and alter speed indexes; and

Monitoring data alerts and respond and resolve these issues.

Reporting data discrepancies and improvement processes achieved in the monthly status report (reference C.5.1.2).

The contractor shall update existing and add new metadata to maintain the integrity ARNG G1 manpower metrics and their relevance to supporting ARNG manpower analysis requirements.

The contractor shall modify stored procedures to incorporate business logic as a result of customer driven changes to policy and practice.

The contractor shall assess and improve the database performance, mod schema, manage indexes, produce roll up tables and views and alter speed indexes in order to provide accurate data which will be forward to end users.

The contractor shall submit an SMMS and RCMS-G System Operations and Maintenance Confirmation Report of Completed Tickets (Section F, Deliverable 18)

C.5.5 TASK 5 – MAINFRAME OPERATIONS

In addition to data sources identified above, the SMMS/RCMS-G system processes data stored on a Pentagon mainframe. The contractor shall perform data operations for these data sources that include the following tasks:

The contractor shall maintain a historical archive of source data files that reside on the Pentagon mainframe. On monthly basis, the contractor shall copy data sets received from SMMS/RCMS-G interfaces to/from the Pentagon mainframe. A process for this bi-directional data push already exists.

The contractor shall provide connections to other systems. This applies primarily to a limited number of situations where the SMMS/RCMS-G interfaces do not provide their data sets directly to SMMS/RCMS-G; rather, these data sources send their data to the Pentagon mainframe and SMMS/RCMS-G pulls these data sources from the mainframe. An example of such an arrangement is the Defense Manpower Data Center (DMDC), which puts Defense Finance and Accounting Service (DFAS) data onto the Pentagon mainframe.

The contractor shall process information, from legacy applications and processes that have not been fully converted to the SMMS/RCMS-G environment. These data sources primarily support the ad-hoc reporting requirement for historical data for legacy systems.

The contractor shall support the management and introduction of changes to the SMMS/RCMS-G Suite.

The contractor shall provide a Mainframe Operations Confirmation Report (Section F, Deliverable 19).

The contractor shall identify and be prepared to eliminate the dependency on the Pentagon Mainframe to perform these tasks within 12 months of time of award.

C.5.6 TASK 6 – SYSTEM INTERFACES

The contractor shall establish and maintain the system interfaces with external modules, systems, applications, and databases. Approximately 40 interfaces exist between SMMS/RCMS-G and external systems. This task is inclusive of adding, modifying, and deleting system interfaces as well as adding, modifying, and deleting supporting system interface agreements.

An interface agreement is valid for one to three years or until a major change occurs. Interface agreements may be called a number of other names such as Interface System Agreement (ISA), Computer Matching Agreement (CMA), or Operational Level Agreement (OLA). Regardless of name, the interface agreement typically includes a background, authorities, security controls, roles, and responsibilities, signatory authorities, points of contact, technical instructions and data file layouts.

The contractor shall accomplish the following tasks:

Change inbound/outbound interfaces to support technology changes, data changes and refreshment;

Develop database schemas and tables to support interface changes;

Populate new tables to support growing product lines within the RCMS-G database;

Establish extracts of data to support requests for information from external systems;

Ensure that all ISAs between RCMS-G and SMMS are properly implemented;

Add new, modify existing and delete obsolete interface agreements as required in the interface lifecycle and;

Output: System Interface Agreement documents shall be archived approximately 40 times per year and shall be updated thirty days prior to the TO expiration. (Section F, Deliverable 20).

C.5.7 TASK 7 – WEB SERVER MAINTENANCE

The contractor shall maintain operational readiness of the Web servers (currently Apache and Internet Information Services (IIS)) that host the SMMS/RCMS-G and SMMS applications. There are currently five web sites hosted on the SMMS/RCMS-G server and three web sites hosted on the SMMS server. The support in this area includes the following tasks:
Ensuring web sites maintained under this contract continue to meet DoD security standards and maintain full accreditation in accordance with the security section of the Program Management Plan;

Ensuring public web sites are registered with the most popular search engines (e.g., Google Bing, Yahoo) to increase visibility, and take actions to ensure web sites private to the SMMS/RCMS-G program are hidden from those search engines;

Ensuring that web applications are scalable to meet the future needs of the ARNG, and that applications make maximum practical use of object oriented design and component reusability;

Planning, coordinating, and conducting web site usability studies;

Ensuring public web sites are registered and take actions to ensure web sites are private to the SMMS/RCMS-G program;

Ensuring that web applications are scalable to meet the future needs of the ARNG and that applications make maximum practical use of object oriented design and component reusability;

Ensuring web sites maintained under this contract continue to meet DoD security standards and maintain full accreditation;

Ensuring web sites, web applications, and data processes are secure and conform to the DoD Risk Management Framework;

Planning, coordinating and conducting web site usability studies and;

Providing a system capable of handling 6,000 concurrent visitors to the public site, conducting routine functions without system degradation.

The contractor shall provide a Web Server Maintenance Confirmation Report of completed maintenance tickets (Section F, Deliverable 22).

C.5.8 TASK 8 – INCIDENT AND PROBLEM ANALYSIS

The incident/problem resolution process involves both the immediate assistance with resolving problems and analyzing issues in order to prevent the reoccurrence of incidents and errors. To increase efficiency of employed systems and to minimize disruption to the on-going operations of SMMS/RCMS-G, the Government is driving the SMMS/RCMS-G program toward a more proactive approach to problem management. This approach relies on the ability to correlate and analyze incident and information from multiple sources including service desk tickets, change requests, alarms generated by automated sources and others. The goal of this approach is to identify potential problems before they actually occur and effectively improve customer service and system performance, while lowering support costs.

The support in this area includes the following tasks:

Performing analysis that leads to the identification of root cause of problems and the means of resolving them;

Completing and submitting the root-cause analysis results, along with recommendations, to the Government for each major event (system warnings and exceptions as defined by the contractor's process), such as an event that results in an outage that cannot be resolved through standard procedure;

Providing recommendations that are technical solutions and incorporate suggestions for improving internal processes and;

Continually performing this analysis and presenting the Government with recommendations.

Creating and managing a database that contains information about known problems and their expected resolution that is consistent with Information Technology Infrastructure Library's (ITIL®) Known Error Database approach and;

Output: Presenting the summary results of the analysis, along with recommendations for improvement, as a part of the Monthly Status Report (Reference C.5.1.3 - Section F, Deliverable 04). The contractor shall provide and Incident and Problem Analysis Confirmation Report of Completed Tickets (Section F, Deliverable 23) Approximately 10,000 help tickets per year shall be expected.

C.5.9 TASK 9 – DEFECT IDENTIFICATION, TRACKING AND RESOLUTION

The contractor shall identify and respond to defects or faults in the SMMS/RCMS-G Suite of applications, modules, performance or function. The contractor can expect approximately 220 corrective maintenance activities per year.

The support in this area includes the following tasks:

Producing and implementing a process to identify, track and resolve defects. This process shall include the development, test, and production environments with identification by Quality Control Testers and/or the developers, as well as field users;

Defining a process to address high impact defects as well as routine defects;

Tracking all defects as service desk tickets and updates information about their status and resolution;

Providing the capability to identify and respond to inquiries of data abnormalities contained within SMMS/RCMS-G data source as it relates to historical data sources. Responses are required within 12 hours and;

Providing the capability to inform Users when any module or application is off line or down for Maintenance or updates.

The contractor shall provide a Defect Identification, Tracking and Resolution report, (Section F, Deliverable 24).

C.5.10 TASK 10 – SMMS/RCMS-G SECURITY SUPPORT AND USER ACCESS

The contractor shall ensure that all access to the SMMS/RCMS-G environment is CAC enabled. The contractor shall ensure that records are tied to the CAC login of the User entering the information in order to send system emails related to the particular record and auditability. The contractor shall implement an enterprise approach to roles and permissions management encompassing all modules, data, and web pages tools. The contractor shall implement single sign on capability for all modules.

C.5.10.1 SECURITY COMPLIANCE

The contractor shall maintain SMMS/RCMS-G environment to meet all DoD system security standards and system accreditation standards as defined by DoD. Assessing Security and Privacy Controls in Federal Information Systems and Organizations is the current standard for selecting security controls in order to meet the Risk Management Framework (RMF) guidelines and all other requirements to continue receiving an Authorization to Operate (ATO) as appropriate.

SMMS and RCMS-G have an RMF categorization of as Medium-Medium-Medium.

Security Controls and inherited from Common Control Providers (CCP) and the Army Policy Record.

The contractor is responsible for Implementing Security Controls, Assessing Security Controls, preparing for System Authorization events, and Monitoring Security Controls on a continuous basis.

The contractor shall ensure security controls selections are updated in order to ensure the system is updated appropriately to reflect DoD Accreditation and security standards. The contractor will ensure at a minimum that SMMS/RCMS-G meets the National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS) and Federal Information Security Management Act (FISMA) guidelines set forth in the latest versions of the following documents which are available electronically under DoD government websites:

- NIST SP 800-53
- NIST Special Publication 800-53A Rev 4 (or current revision)
- FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems
- NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347
- NIST 800-129 Guide for Security-Focused Configuration Management of Information Systems
- NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems
- FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems
- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
- DoDI 5000.2, Operation of the Defense Acquisition Systems

The contractor shall document both, system security processes and any security incident or threat in the security section of the Program Management Plan. The contractor shall comply with DoD SOP requirements for compromised data breach as listed DoDD 5400.11-R (DoD Privacy Program) and relevant DoDI for policies, and required actions.

The support in this area includes the following tasks:

1. Ensuring SMMS/RCMS-G application is programmed according to DISA Security Technical Implementation Guidelines (STIGs), SRG, and will run in an environment and on servers that are STIG/Unified Gold Master (UGM) compliant;

2. Validating configurations with an approved Security Content Automation Protocol (SCAP) scanner and provide scan results as eMASS artifacts and provided as requested;

3. Performing vulnerability scans and reviews to identify all patches and updates;

4. Providing automated daily vulnerability assessment and reporting based on asset inventory;

5. Automatically scanning the environment, source code, and stored procedures to identify and remediate vulnerabilities;

6. Automatically generating service tickets for detected vulnerabilities;

7. Aggressively mitigating vulnerabilities to prevent loss of capability, performance, or information;

8. Providing the security-related support for patch management to include: Testing all security patches provided by the industry and the DoD to ensure they do not have negative impact on the operational systems;

9. Reviewing waiver requests and present recommended actions to the ARNG TPOC;

10. Adding, updating, and deleting system level user accounts for privileged access of government accounts; and

11. Removing dormant accounts based on business rules.

The contractor shall maintain a FISMA compliance with no CAT I (30 days to remediate), CAT II (60 days to remediate) and CAT III (90 days to remediate) vulnerabilities or have a POA&M in place to mitigate findings within compliance windows (Exploitable vulnerabilities must be mitigated instead of placed on a POA&M). Vulnerabilities are not considered remediated until they are eliminated from the training and production environments.

The contractor shall update eMass to reflect the status of security control and vulnerability scans.

The contractor shall be responsible for maintaining security control documentation, associating it to controls in eMASS and making it available upon request by the AO, ISO, ISSM, ISSO, or an outside agency.

The contractor shall monitor Authority to Operate (ATO) records for all SMMS/RCMS-G modules and support the Plan of Action and Milestones (POAM) as initiated by the Government. The contractor shall update eMASS instances to reflect system status.

Output: The contractor shall provide an in process review in the Monthly Status Report (Reference C.5.1.2).

C.5.11 TASK 11 – CYBER SECURITY MONITORING

The contractor shall work with Cyber Security Service Providers (CSSP) and other 3rd parties to monitor and respond to cyber threats.

The contractor shall:

1. Support 3rd party Security Control Assessments and Validations (SCA-V);

2. Perform vulnerability assessments in order to prepare for and in support of systems Security Control Assessments and Validation events;

3. Perform RMF or current DoD standards assessments of the SMMS/RCMS-G;

4. Perform source code and executable scans of the SMMS/RCMS-G system and ensure that the system meets all NIST and DoD security requirements;

5. Monitor and respond to Information Operations Condition (INFOCON) Levels to comply with the SD 527-1 or current standard required baseline. When the INFOCON level is elevated, document the level change, the needed readiness activities, the completion of those activities, and any issue associated with complying with the INFOCON required steps;

6. Review and identify recommendations for Chief Technology Officers (CTOs), Execution Orders (EXORDS), including necessary waiver requests and POAMS and deploy guidance and procedures for all INFOCON levels and transitions between them;

7. Support implementation of the emerging cyber warfare doctrines, as required;

8. Update documentation and systems such as e-MASS to reflect system compliance with security controls, architecture, etc.;

9. Ensure the environment maintains accreditation under the Risk Management Framework (RMF) accreditation and all other requirements to continue receiving a Tenant in Good Standing Certificate and/or Authorization to Operate;

10. Contractor shall ensure that the Army HBSS, SCCM and Antivirus clients are installed and functional; and

11. Output: The contractor shall provide an in process review in the Monthly Status Report (Reference C.5.1.2).

C.5.12 TASK 12 – DATA OPERATIONS

The contractor shall utilize the Kimball Data Warehousing Methodology to support SMMS/RCMS-G data operations.

Data Pre-Processing: The purpose of data pre-processing tasks is to ensure that the date set files received by the SMMS/RCMS-G and SMMS are valid and complete. ARNG defines “valid data” as data that conforms to the expected data characteristics as defined in the destination tables and does not deviate from the historical patterns.

The contractor shall:

1. Receive data from the external sources. Most interfaces require daily data updates. These interfaces are already established with automated processes (see Task 6 for Systems Interface Requirements);

2. Ensure that all expected data sources have delivered their data (via automated data feeds) by the time agreed-upon in the corresponding agreements;

3. Conduct pre-processing of external data feeds to ensure that record counts and file structures are consistent with previous data feeds;

4. Run a series of automated quality control processes on each new data set to identify record count and characteristics abnormalities and raise alerts if it appears that any inconsistencies exist;

5. Store copies of verified source data in the staging SMMS/RCMS-G databases;

6. Conduct pre-processing of external data feeds to ensure that record counts and file structures are consistent with previous data feeds as a quality control measure;

7. Load pre-processed data into the SMMS/RCMS-G production data store; and

8. Provide the capability to store copies of verified source data in the staging SMMS/RCMS-G databases.

C.5.12.1 DATA PROCESSING

The purpose of data processing tasks is to ensure that the data set files received by the SMMS/RCMS-G are properly inserted into the existing SMMS/RCMS-G tables.

The contractor shall:

1. Create data sets for inclusion into the SMMS/RCMS-G data stores, by removing data duplications as identified by the system. Only data records that represent a change or new records shall be appended to a historical database for the life of the system thus supporting accurate backward and forward time series analysis and comparisons;

2. Load pre-processed data into the SMMS/RCMS-G production data store; and

3. Close records that need to be closed based on existence of updated records in the source data. SMMS/RCMS-G never replaces any records; rather old records are closed and new records are inserted. For example, if a soldier is promoted, a new record with the promotion information is inserted into the database and the old record is “closed” by populating “end date” of the previous rank

C.5.12.2 DATA PROCESSING ERROR RESOLUTION

1. As issues with the incoming data are identified, the contractor shall:

2. Identify and/or respond to inquiries of data abnormalities contained within SMMS/RCMS-G source data, especially as it relates to the historical data sources;

3. Identify and carry out corrective actions to resolve data abnormalities;

4. Create ad hoc reports using various tools including MS Excel, SQL and MS PowerPoint and other tools to communicate data issues with ARNG leadership and functional experts; and

5. Create resolution methodologies that will minimize data anomalies and invalid or missing data.

C.5.12.3 DATA QUALITY

The contractor shall:

1. Maintain and change existing automated data quality control processes by verifying and validating anomalies;

2. Use historical information as the basis for conducting analyses to determine if the new data sets are within an acceptable range and meet expected characteristics;

3. Develop metrics using background statistics and linear regression analysis to determine the validity of the data;

4. Perform periodic data checks on the metrics to identify any data abnormalities;

5. Inspect abnormalities in the metrics to determine if the change is expected or might be signaling an anomaly that may exist;

6. Create data sets for inclusion into the SMMS/RCMS-G data stores by removing data duplications as identified by the system;

7. Create resolution methodologies that will minimize data anomalies and invalid or missing data;

8. Identify and carry out corrective actions to resolve data abnormalities and report abnormalities to user;

9. Inspect abnormalities in the metrics to determine if the change is expected or might be signaling an anomaly that may exist;

10. Maintain and change existing automated data quality control processes by verifying and validating anomalies; and

11. Perform periodic data checks on the metrics to identify any data abnormalities.

C.5.13 TASK 13 – CONTINUITY OF OPERATIONS PLAN/DISASTER RECOVERY OPERATIONS

SMMS/RCMS-G COOP arrangements fall under the general COOP policies and procedures in use by the hosting center. In general, any updates to the production systems are automatically replicated to the COOP site. The COOP site for SMMS/RCMS-G is procured and hosted by the Government and the Government purchases all hardware and software needed to maintain the alternate COOP site. Under this contract, the contractor shall ensure that all the equipment at the alternate COOP site is configured identically to the maintained equipment at the locations that support the primary SMMS/RCMS-G environment. The contractor shall verify that every change to the production environment is reflected in the COOP environment within 24 hours.

The contractor shall test the COOP and disaster recovery systems and operational plan at least once during the Base Period of the contract and once during each Option Period of the contract.

During a state of emergency, the contractor shall supply essential personnel as identified in the Information System Contingency Plan (ISCP); The SMMS/RCMS-G ISCP establishes comprehensive procedures to recover SMMS/RCMS-G quickly and effectively following a service disruption. Essential personnel are identified as contract support personnel in support of the ISCP. Depending on the type/level of crisis, these personnel will begin communication immediately with the SMMS/RCMS-G System Owner to ensure recovery and operations of the system in accordance with the ISCP.

The contractor shall ensure that all systems within the alternate COOP facility are ready to take over operations from the systems located at the primary location for SMMS/RCMS-G environment within Recovery Time Objective (RTO) and Recovery Point Objective (RPO) limits after primary system's failure. This requires the contractor to ensure that the alternate COOP systems:

1. Recovery Time Objective (RTO) is 4 hours. Recovery Point Objective (RPO) is 72 hours;

2. Have the same software release levels and patches as the primary SMMS/RCMS-G systems;

3. Are configured with the same configuration information as the primary systems; and

4. Are capable of operating on their own in case of partial or complete failure of the primary systems.

The contractor shall (in coordination with the government) develop and maintain a COOP and ensure the COOP Plan is coordinated with the TPOC and ARNG G6 in order to ensure system operation in the event primary system infrastructure becomes inaccessible.

The contractor shall:

1. Evaluate the technologies and services available at hosting environments to determine the most cost effective means to meet RTO and RPO limits;

2. Review and provide recommendations to the government on changes to COOP and Disaster Recovery to the Government on an annual basis. Recommendations will include technical details, costs, and RTO/RPO projections;

3. Identify and report to the government the resources required to implement COOP operations;

4. Supply essential personnel as identified in the Information System Contingency Plan (ISCP) in support of a state of emergency;

5. Maintain a Continuity of an Operations Plan (COOP) that is coordinated with the ARNG G6 in order to ensure that all systems will be operational during any of the events that will trigger a COOP operation;

6. Maintain the environment and applications at production and COOP locations;

7. Verify that every change to the production environment is reflected in the COOP environment within 48 hours of final user acceptance;

8. Ensure that all the equipment at the alternate COOP site is configured identically to the maintained equipment at the locations that support the primary SMMS/RCMS-G systems; and

9. Ensure the SMMS and RCMS-G systems' pre-production and production environments are documented in build guides so that the environments and systems can be rebuilt as necessary.

Essentially, the contractor is required to be readily available in performance of this task.

The contractor shall provide a COOP (Section F, Deliverable 25) 30 days from task order award.

C.5.14 TASK 14 – DATA REPROCESSING

Based on historical records, the ARNG anticipates that a small percentage of the data obtained from the external sources will have corruptions that cannot be identified using the standard check and data quality control processes discussed above. These issues are caused by mistakes introduced by the owners of the data feeds. When notified of such issues the contractor shall:

1. Work with the owner of the data source to create methods for identifying the corrupted elements in the SMMS/RCMS-G staging database and update the affected records to their correct values;

2. Rerun all standard checks and quality control processes and reload the updated data into the SMMS/RCMS-G data store following the data fixes to the staging area;

3. Keep historical records of all such events, including at minimum, information about the data source, issues, affected date range, fields, and steps taken to resolve the problem;

4. Evaluate these events for inclusion into the standard data verification and quality control processes; and

5. Deliver the results of this analysis and the details about each event to the ARNG as part of the Monthly Status Report (Reference C.5.1.2).

C.5.15 TASK 15 – STANDARD REPORT GENERATION AND DISSEMINATION

The contractor shall ensure that all standard reports are generated, verified, and delivered to the recipients in a prearranged manner. Standard reports are reoccurring reports with the same data elements with format provided by the government.

The contractor shall:

1. Use statistical sampling methods to verify accuracy of the reports;

2. Ensure that all reports and data files have been delivered by the agreed upon date and time;

3. Ensure that all pre-scheduled reports have run and can be accessed;

4. Ensure correctness of the reports in terms of format and integrity of data; and

5. Create raw data sets, using either manual or automated process, for delivery to recipients.
6. The contractor shall update standard reports monthly and upon request. All monthly reports are due by the 10th calendar day of each month (if the 10th day falls on a weekend/federal holiday, the report is due the last business day prior to the weekend/federal holiday). Complex data requests requiring the assistance of technical support will be initiated within 24 hours of receipt, and timelines for completion shall maintained in accordance with the timelines developed during the change management process.

All reports must be completed/packaged according to the corresponding formats provided by ARNG, OUSD (P&R), DAPE-MP, regulatory and statutory guidance. At any time, OUSD (P&R) or DAPE-MP can changed the format, reporting dates, or add or delete reports (Reference Section J, Attachment G).

C.5.16 TASK 16 – AD HOC QUERIES AND REPORTS

The Government requires ad hoc queries and reports to be created each month. The tables below provide data on the number and structure of these queries and reports. The contractor is expected to produce no more than 160 ad hoc queries per month (Section F, Deliverable, 27). Each Ad Hoc Report shall be tested and verified before providing the report to the Government. The information shown is based on historical data; the size and structure of the queries and reports may vary in the future. Ad hoc reports are reoccurring reports with the same data elements with format provided by the Government.

Type of Effort	System impacts
Small	Current data and systems

Medium	Minor system changes
Large	New Government data and/or significant system software maintenance/changes

Table 1 - Level of Effort Required for Ad Hoc Queries and Reports

Priority of Effort	Response Time
High	Less than 4 hour turn around
Medium	24 hour turn around
Low	96 hour turn around

Table 2 - Priority Levels for Ad Hoc Queries and Reports

C.5.17 TASK 17 – CHANGE AND CONFIGURATION MANAGEMENT SUPPORT

Change Management focuses on how any change in the system is determined. The change management system incorporates activities such as identification of changes, impact analysis of changes, documentation of change requests (CRs), Change Control Boards (CCB), communications to stakeholders and implementations of approved CRs. All CRs require the TPOC's signature prior to entering the Change Implementation process (see C.5.16 -Task 16).

Configuration Management focuses on how any change to the system should be performed. The Configuration Management Database (CMDB) is the central to the process of Configuration Management. The CMDB includes information about the system's hardware and software as well as relationships between assets. The CMDB displays this information over time and can be used for activities such as root cause analysis, impact analysis, and Change Management.

C.5.17.1 CHANGE MANAGEMENT

The contractor shall be responsible for delivering the Change Management Plan within 30 days of time of task order award (Section F, Deliverable 28). The contractor shall operate the Change Management process throughout the contract to include Change Request collaboration and creation and management of the Change Control Board.

The SMMS/RCMS-G has three levels of changes to the application as described below:

Type of CR	Change Criteria	Estimated Number of Changes Annually
Minor Change Request (MCR)	Minor impact on requirements with no impact on infrastructure or environment 5 Business Days to develop change management documentation and initial estimate (e.g., change in icon color, changing metric)	1,950

System Change Request (SCR)	Minor to moderate impact on requirements with no impact on infrastructure or environment 15 Business Days to develop change management documentation and initial estimate (e.g., product changes, new report capability)	175
Engineering Change Proposal (ECP)	Minor to major impact on requirements and may impact infrastructure or environment. 30 Business Days to develop change management documentation initial estimate (e.g., major system changes)	6

Table 3 - Type and Frequency of Change Requests

C.5.17.2 CONFIGURATION MANAGEMENT

The contractor shall:

1. Review information already stored in the CM tool for accuracy and applicability;

2. Manage and maintain processes associated with bringing new systems, or changes to the existing systems, into the operational environment, including maintaining engineering library of software/hardware releases (code, hardware configuration, load builds, scripts, design documents, etc.);

3. Assist in SMMS/RCMS-G system testing and integration;

4. Measure impact of changes on the users;

5. Update existing or create new Configuration Management Plan/ SOPs as required by the changes to the existing systems or introduction of new system components;

6. Coordinate CM-related functions with other ARNG organizations and assist as requested in enterprise CM support;

7. Update CM information as needed;

8. Create and maintain detailed diagrams (as built) of the existing SMMS/RCMS-G infrastructure and systems in order to conduct O&M activities;

9. Perform daily scans for assets not in asset inventory. CruiseControl.NET, an Automated Continuous Integration server, is currently implemented using the .NET Framework to ensure that all products are using the latest versions available. Other tools that meet the requirement may be used to conduct the scans;

10. Perform license utilization analysis and present the ARNG with appropriate recommendations for corrective action, i.e., removal, purchase of additional licenses; and

11. Create means of making the ARNG aware of assets that require maintenance renewals within six months.

In order to conduct O&M activities for SMMS/RCMS-G, the contractor shall create a means of retrieving the license and maintenance agreement information via a user initiated report against the CMDB data. An authorized user shall be able to initiate and view the resulting reports using any standard Web browser.

C.5.17.3 CHANGE IMPLEMENTATION

The SMMS/RCMS-G is constantly changing and expanding. This expansion is primarily driven by: (a) availability of new data elements, (b) user requests, (c) technology evolution, and (d) ARNG mandates.

To support this expansion and changes, the contractor shall:

1. Provide technical resources and capabilities to change existing and implement new business logic and to update and change the SMMS/RCMS-G environment and its offerings;

2. Create and verify fields and metrics; and

3. Create new metrics (metadata and equations) to support new features, add new data sources or data versions, and making changes to SMMS/RCMS-G products.

The contractor shall be responsible for delivering the Configuration Management Plan within 30 days of task order award (Section F, Deliverable 29). The contractor shall demonstrate a working Configuration Management Database within 60 days of task order award (Section F, Deliverable 30). The contractor shall take the following precautions while engineering changes:

1. Document dependencies as they become known;

2. Create test scripts to test all changes. Test scripts may be manual or automated;

3. Exercise test scripts for all major components after any system deployment;

4. Use Training Application for all tests before deployment to Production Application;

5. Create system rollback points prior to implementing new changes;

6. Advise the Government within 24 hours of a self-inflicted error and document the dependency to avoid future instances of creating the same error;

7. Change work shall not begin without COR concurrence;

8. Change SMMS/RCMS-G functionality as mandated by DoD, Active Component, and ARNG manpower and human resource management policy changes;

9. All changes shall follow the change management process. These solutions require implementation of good software change practices;

10. Implement dual directional data interfaces between SMMS/RCMS-G and Integrated Personnel and Pay System Army (IPPS-A). Support data calls and testing of interface to IPPSA system to ensure that the required system interfaces between SMMS/RCMS-G and IPPSA provides accurate incoming and outgoing requirements; and

11. Modify and optimize the SMMS/RCMS-G product, module, and model suite: Modify and optimize the SMMS/RCMS-G Suite to integrate with new operating systems, compilers, system utilities, and other system products as well as operate the Configuration Management process throughout the contract to include identification and labeling of configurable items, maintenance of configurable items, configuration verification and auditing with records auditable over time.

C.5.17.4 CONFIGURATION IMPLEMENTATION

An approved CR enters the Change Implementation process. The contractor shall implement changes to the system as identified in the Change Management process. To support Change Implementation the contractor shall:

1. Add, modify and delete code and business logic to implement changes;

2. Add, modify and delete data metrics in the data warehouse;

3. Add, modify and delete source code from a repository with branches dedicated branches for testing, development and production code;

4. Modify the system environment as required to implement change (inclusive of adding, modifying or deleting external data feeds);

5. Create test scripts for user acceptance testing;

6. Conduct user acceptance testing, regression testing, unit testing and other types of testing as required to implement the change;

7. Update system documentation after changes are implemented;

8. Summarize system changes completed on the Monthly Status Report (Reference Section C.5.1.2).

9. Maintain and change the SMMS/RCMS-G test strategy that includes unit, integration, system, and acceptance testing from both a top-down and a bottom-up approach. This strategy identifies data or software issues which, if not resolved, may threaten accuracy and operational status of SMMS/RCMS-G;

10. Develop and use System/Software Testing Checklists as outlined by the Software Test Plan to document testing of changes, or new developments. Testing shall include unit, integration, system, and acceptance testing from both a top-down and a bottom-up approach;

11. Test all changes and changes prior to implementation to prevent the occurrence of any potential problems in products, modules, models, or systems and;

12. Maintain and report testing artifacts, including defect types, status, and resolution.

The ARNG will define specific change efforts based on information brought forward by internal and external stakeholders.

C.5.18 TASK 18 – HELP DESK / SERVICE DESK INFRASTRUCTURE

The contractor shall establish a service desk. (Reference Section J, Attachment H)

The Service Desk Infrastructure shall include:

1. Service Desk Ticketing System,
2. Service Desk Call Reporting System,
3. Service Desk Ticket Creation, and
4. Service Desk Managing Tickets.

The contractor shall provide verifiable closed tickets on a daily basis (Section F, Deliverable 31).

C.5.18.1 SERVICE DESK TICKETING SYSTEMS

This contractor-provided ticketing system shall be used to track and manage user inquiries as well as events reported though automated systems (Simple Network Management Protocol (SNMP) alerts, etc.). In addition, the system must be able to track projects and their approval process.

System must generate the following minimum set of time stamps for each ticket record:

1. Create date and time;
2. Last updated date and time;
3. Resolved date and time; and
4. Closed date and time.

The Service Desk shall be located at the contractor's facility.

The contractor shall provide and manage a ticketing system, which will be used to manage incident, problem and service requests reported by the users, SMMS/RCMS-G staff (Government and contractor), or automated sources.

To support service desk operations, the contractor shall provide:

1. Assistance with account issues;

2. Assistance with usage of the SMMS/RCMS-G Suite and its features;
3. Troubleshooting;
4. Coordination of resolution efforts; and
5. Grant access to government program management team to perform reporting and analysis.

C.5.18.2 SERVICE DESK CALL REPORTING SYSTEM

Service Desk Call Reporting Requirements:

The contractor shall provide a Web-based SD call reporting system capable of presenting real time and historical data about call, email, and Web activities.

The contractor provided repository shall be capable of transmitting the above information to a standards based external database using SQL, Java Database Connectivity (JDBC), and/or Open Database Connectivity (ODBC) interfaces

The reporting tool shall have the flexibility to collect data and distribute reports via 'push' or 'pull' method, or a combination thereof.

The Call/Contact Type reports shall, at a minimum, include the following types of data for each call type:

1. Average and longest speed of answer;
2. Service levels;
3. Number of calls, offered, answered and abandoned;
4. For inbound calls (on a per hour, per 30 minute, and Busy Hour basis);
5. Average Speed To Answer;
6. Average Talk Time;
7. Average Wrap Up Time;
8. Average Hold Time;
9. Abandon Rate;
10. Longest Wait Time;
11. Longest Talk Time;
12. Number of received and associated response times for email requests;
13. Number of received and associated response times for Web requests; and
14. Categorization of ticket priority as Critical, Normal, or Low.

Outage Notification:

The contractor shall be responsible for:

1. Communicating information about known outages to the users and other support organizations;
2. Communicating scheduled maintenance notification at least 48 hours in advance; and
3. Communicating information about known issues and their anticipated resolution times.

The contractor shall ensure that its notification about unscheduled maintenance is posted no less than 15 minutes before the start of the maintenance.

C.5.18.3 TICKET CREATION

The contractor shall use standard, compliant, database for storage of all tickets and supporting information. Support implementation of workflows associated with:

1. Escalation of tickets (automated assignment to an organization, or generation of alerts based on logically-defined and time parameters);
2. Staff involved in the escalations and approval process must be alerted via email that an action is required within specified time frames; and
3. Support a hierarchical ticket classification scheme as specified in the contractor's SOP.

The contractor shall ensure that each ticket record contains the minimum set of fields, which includes:

1. Type of ticket (incident, problem, request, etc.);
2. Work log (log of steps taken in resolving the ticket);
3. Each entry shall have a time stamp and ID of the person making the entry;
4. User's name and contact information;
5. Multi-level classification scheme;
6. Ticket Status; and
7. Assignment.

Ticket Creation Requirements: The SMMS/RCMS-G Service Desk is operated and maintained by the contractor and the contractor shall provide support to the users of the SMMS/RCMS-G Suite and its products. All calls from the users are routed to the Service Desk for initial handling. To handle incoming calls, the contractor shall:

Provide live telephone coverage from 8:00 am to 8:00 pm Eastern Time each week day - Monday through Friday, excluding Federal holidays.

The contractor shall:

1. Answer calls and greet the customer with a standard welcome message as provided by ARNG;
2. Verify existing or obtain new user information;
3. Identify the nature of the problem and classify it correctly;
4. Record any additional information obtained from the user;
5. Assign priority as defined by service desk operations procedures; and
6. Provide the user with a ticket number.

To handle emails and Web submissions, the contractor shall:

1. Review email and Web request queues in regular intervals Monday through Friday 8:00 am to 8:00 pm Eastern Time, excluding Federal holidays;
2. Create tickets for each email and Web request; and

3. Contact user with ticket number.

Available statistics indicate an average call-length of seven minutes. Over a recent one year period, the call distribution was as follows:

Time of Day of Ticket Creation	**Number of Calls**
8:00 am – 9:00 am	1,465
9:00 am – 10:00 am	1,548
10:00 am – 11:00 am	1,800
11:00 am – 12:00 pm	1,786
12:00 pm – 1:00 pm	1,496
1:00 pm – 2:00 pm	1,441
2:00 pm – 3:00 pm	1,387
3:00 pm – 4:00 pm	1,347
4:00 pm – 5:00 pm	988
5:00 pm – 6:00 pm	618
6:00 pm – 7:00 pm	51
7:00 pm – 8:00 pm	1
Total	14,385

Table 4 - Average Daily Service Desk Calls by Hour

C.5.18.4 MANAGING TICKETS

To manage tickets created by or assigned to the contractor, the contractor shall:

1. Maintain status of all open tickets and escalate as required;
2. Coordinate resolution with other internal and external teams, as appropriate;
3. Update the users with progress of the incident resolution through the ticket and; updates.

The contractor's staff shall own the problem resolution process from the initial contact with the users to resolution of the incident regardless of whether the problem is resolved within SD or it has to be escalated to other organizations. To ensure that the users are updated with the progress of the resolution process, the contractor's staff shall provide updates to the users on a regular basis. The contractor's staff shall also be responsible for verifying resolutions with the users, by doing regular checks with ticket submitters of a subset of resolved tickets, to verify user concurrence in the resolution. These checks shall take place on a monthly basis.

The contractor's personnel shall not reject a caller based upon a problem not being within their purview. The contractor shall make every effort to refer it to the most appropriate support organization. Support organizations may include external data partners, cloud help desk, ARNG IT Help Desk, or other external support organization best suited to handle the caller's issue.

C.5.19 TASK 19 – ANALYTICAL SUPPORT

The contractor shall provide analytical support for analysis of issues related to achieving and maintaining personnel readiness objectives and ad hoc responses to a wide range of complex questions raised by external and internal organizations.

The contractor shall make recommendations to the Government to most effectively integrate the diverse sources of data in SMMS/RCMS-G and to categorize/define the issues and problems that meet ARNG policy needs.

The contractor shall provide a limited number of personnel supporting analytics functions located at the Temple Army National Guard Readiness Center (TARC) located in Arlington, Virginia to provide analytical support services. This support averages 3-5 personnel per period of performance. The contractor assigned analysts shall:

- Applying objective, analytical, and orderly thinking to the analysis of complex operational and management problems, and supporting this analysis when appropriate with the use of tools and techniques such as statistical inference, models, mathematical programming, and simulations
- Conduct studies, research and prepare reports for executive level presentation
- Address specific data extraction and manipulation requirements
- Identifying and formulating solutions to problems ranging from minor data quality issues to strategic forecasting of future personnel trends
- Conducting qualitative and quantitative analyses of complex military personnel and readiness issues
- Summarizing and synthesizing complex analyses into simplified terms for presentation to decision makers
- Integrating techniques into operational processes and algorithms used in the daily data preparation and quality control of the data warehouse
- Provide results in a Monthly Ad Hoc report, (Section F, Deliverable 32)

C.5.20 TASK 20 – PROVIDE SMMS/RCMS-G LIASION SUPPORT

The contractor shall designate SMMS/RCMS-G liaisons of total staff for each SMMS/RCMS-G product, module, model, and prototype to interface with the ARNG POCs and user community. Each SMMS/RCMS-G liaison may handle multiple SMMS/RCMS-G products.

On a day to day basis, contractors serving as liaisons shall be responsible for:

1. Work with ARNG POCs to determine, recommend, prioritize and verify implementation of adaptation, maintenance, and change efforts;
2. Maintain continuous communication with ARNG POCs for program policy and implementation of the SMMS/RCMS-G products, modules, and models;
3. Convey requirements between government module functional owners and the contractor's program management team; and
4. Assist government functional module owners with the change management process.

Organization Supported
Strength Maintenance (HRR)
Human Resource (HRM)

Personnel Systems (HRP)
Soldier and Family Support (HRS)

Table 5 - Liaison Support

C.5.21 TASK 21 – ENGINEERING SUPPORT

The contractor shall provide engineering support to meet the changing needs of the SMMS/RCMS-G user community, maintain industry best practices, and plan for long-term growth and sustainability of the SMMS/RCMS-G Suite. The contractor shall identify potential projects to improve SMMS/RCMS-G capabilities and engineering changes needed to meet program objectives. The contractor shall perform additional engineering initiatives, to support changing technologies or are based on emerging requirements identified by the ARNG.

Engineering support shall include:

1. Providing technical improvement recommendations to ongoing SMMS/RCMS-G O&M efforts;

2. Anticipating changes in the SMMS/RCMS-G technical and business requirements and making recommendations implementing industry best practices;

3. Providing technical and business recommendations to support the SMMS/RCMS-G strategic planning process;

4. Assessing impact of changes to SMMS/RCMS-G requirements on technical and cost baselines;

5. Any changes or engineering support that become a requirement by a change in law, regulation, or policy that are not covered in the scope of this contract shall be; coordinated through the COR/CO for approval and contract modification

6. Providing ongoing coordination with software maintenance team(s) for tailored products, modules and models database and best practices support as provided by users to make engineering revisions;

7. Preparing, planning, and migrating hosting of the SMMS/RCMS-G and SMMS Development, Testing, and Production environments to a FEDRAMP approved DoD Cloud Service Provider (CSP) as directed by the government and;

8. Migrating capabilities into a common solution.

C.5.22 TASK 22 – STANDARD OPERATING POLICIES AND PROCEDURES

The contractor shall establish and maintain formalized Standard Operating Policies and Procedures (SOPs) and operational plans for each process that supports the operation and maintenance of SMMS/RCMS-G.

The contractor shall deliver these (new or updated) procedures for review and approval by the Government. Standard operating procedures include:

1. Service Desk and On-site Support; including ticket creation, updates and resolution;
2. Onboarding, account creation and provisioning;
3. Disaster Recovery Plan;
4. Continuity of Support Plan/IT Contingency Plan;
5. Crisis Communication Plan;
6. Cyber Incident Response Plan;
7. Backup, Archive, and Recovery;
8. Data Processing Guide;
9. Information Security and OPSEC;
10. Cloud Resource Management; and
11. Change management plan.

All SOPs shall be delivered to the Government within 60 days after contract award and the contractor shall brief the Government within five business days of the delivery (Section F, Deliverable 33) prior to acceptance of the SOP by the Government.

The contractor shall update these plans and procedures within 30 days of identifying a change (Section F, Deliverable 34) and the Government reserves the right to reject an SOP if it does not meet the mission requirements. If rejected the contractor shall resubmit any rejected SOP within 10 business days for reconsideration.

C.5.23 TASK 23 – DEVELOP OPERATING LEVEL AGREEMENTS

Working with Other ARNG support contractors: ARNG employs services of multiple contractors and Vendors in support of its operations.

The contractor shall work with these entities and establish working agreements (e.g., OLAs) as needed that enable them to provide support that meets the requirements under this PWS.

ARNG will assist with coordinating the interactions between the SMMS/RCMS-G contractor and the other support contractors as needed.

There are approximately 50 contractors and other organizations that the SMMS/RCMS-G contractor shall:

1. Coordinate required to work with other contractors and Government organizations operating within the ARNG; and

2. Maintain and update agreements (Interconnect System Agreements, Memorandums of Agreement, OLAs, and Data Usage Agreements) as required with other contractors and Government organizations to ensure functionality with current and future military personnel systems.

C.5.24 TASK 24 – SMMS AND RCMS-G SYSTEMS MAINTENANCE

The contractor shall maintain each of the SMMS/RCMS-G modules to ensure that they perform in accordance with the specified functional and performance characteristics as defined in the documentation for each module (Reference Section J, Attachment I).

Each module, the contractor shall:

1. Ensure the capability to upload, store and make edits to program policies;

2. Provide the capacities to view the definition of any code by hovering over the code with the mouse clicker;

3. Use common look up tables where possible to minimize the number of locations requiring updates;

4. Ensure access requests and approved use DD Form 2875 thru the User Management tool.

5. Ensure the DD form 2875 (Section J, Attachment J) is updated annually (Section F, Deliverable 35); and

6. Add, modify and delete database metrics

C.5.25 TASK 25 – CLOUD MIGRATION

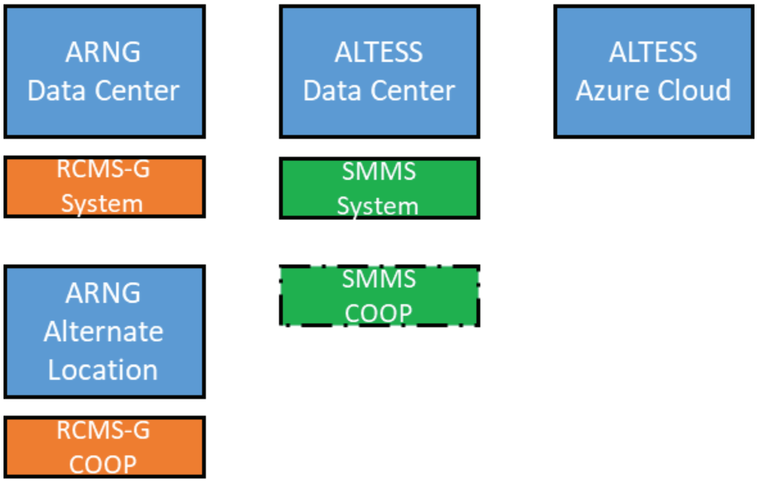
Cloud migration as a task is a single service. The contractor shall develop and execute a plan to transfer hosting of the system to a DOD Cloud Service Provider (CSP) upon notification from the Government.

Neither SMMS nor RCMS-G is currently on a cloud environment but both are in the process of evaluating hosting environments for an eventual move. The contractor shall be prepared to conduct the migration of RCMS-G and SMMS to a FEDRAMP approved CSP.

The contractor shall assume project management activities of the cloud migration task with the systems conducting Configuration 1 through 4 in phases:

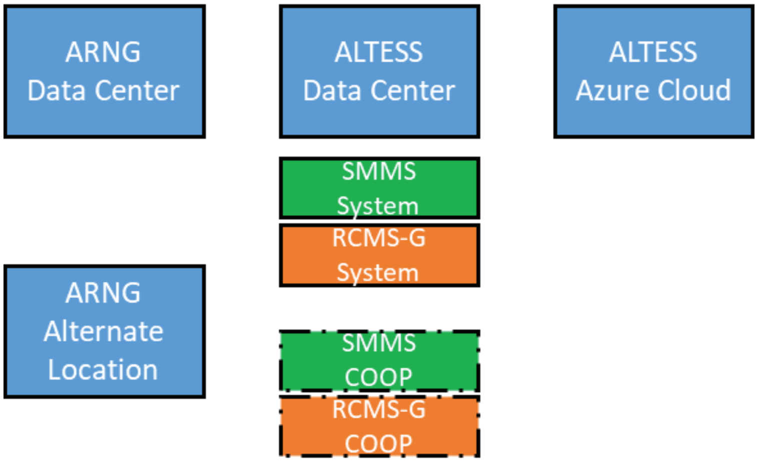
In Configuration 1, SMMS is hosted at the ALTESS Data Center, RCMS-G is hosted at the ARNG Data Center (Installation Processing Node) and the RCMS-G COOP is at the ARNG alternate location.

Configuration 1: SMMS is at ALTESS and RCMS-G is at ARNG IPN



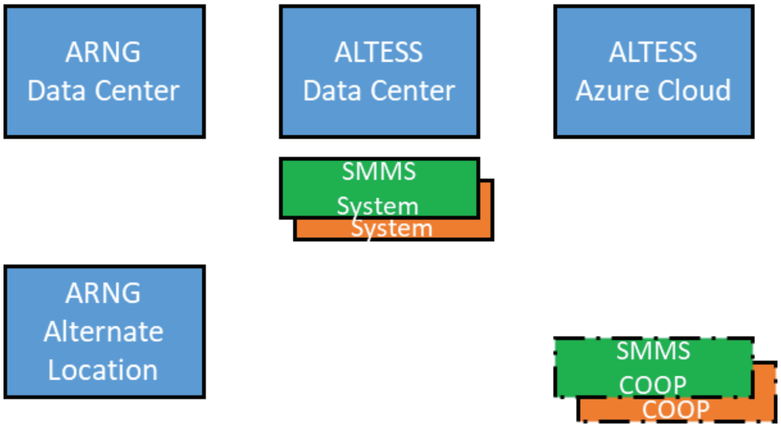
In Configuration 2, RCMS-G is co-located with SMMS at ALTESS.

Configuration 2: SMMS and RCMS-G are at ALTESS



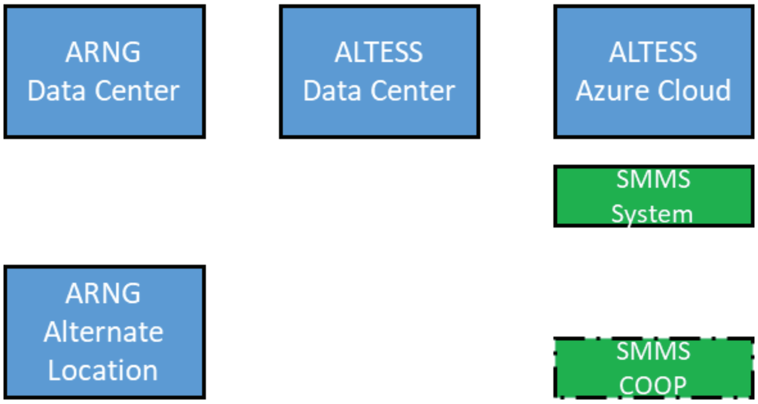
In configuration 3, RCMS-G capabilities are converged into SMMS at the ALTESS and prepared to move into the ALTESS Azure Cloud.

Configuration 3: Converged SMMS at ALTESS



In Configuration 4, a converged SMMS is on the Azure Cloud environment and is able to take advantage of multiple availability zones for redundancy (COOP).

Configuration 4: Converged SMMS at Azure Cloud



Regardless of system location and status under each phase, the contractor shall achieve four goals for each configuration. These goals include:

1. Complete cyber security requirements;
2. Configure modules, applications and system artifacts for operation;
3. Ensure internal and external data feeds and data processing continue on schedule; and
4. Operate a functional COOP and Disaster Recovery plan.

The contractor shall adopt and maintain administrative, technical, and physical safeguards and controls that are required for the security level and services being provided, in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time of contract award) found at http://iase.disa.mil/cloud_security/Pages/index.aspx (Note: the new cyber incident reporting requirements of SRG section 6.4 become enforceable by the Government upon the effective date of the information collection governing the new reporting requirements (see DFARS case 2013-D018). However, this does not abrogate, limit, or otherwise affect the contractor's obligation to comply with any other cyber incident reporting or other reporting requirement that is contained in this contract).

The contractor shall comply with, and enforce IA Workforce standards/ IAT Levels of baseline certifications for the Cybersecurity workforce to include computer environment certifications as applicable.

The contractor shall deliver to the Government or any successor contractor, all system data, to include all code, software, and tools necessary to maintain the cloud hosted environments without interruption upon the conclusion of performance or at the request of the government.

The contractor will also be responsible to:

- Perform code scans as outlined in Task 3 to ensure code and data moved to the cloud environment is compliant with CSP and cloud environment standards and comply with Application Security Development (ASD) STIG;
- Evaluate SMMS/RCMS-G and SMMS to ensure it will be supported in the designated cloud environment;
- Modify SMMS/RCMS-G and SMMS as necessary to transition to the designated cloud environment;
- Implement all applicable security controls with a continuous monitoring plan IAW National Institute of Standards and Technology (NIST) Risk Management Framework and DoD standards;
- Maintain logically segregated development, testing, and production environments/enclaves;
- Provide hosting and backup services for Web, Mobile and IVR platforms. Service will include, as required by RMF, a secondary, redundant, independent infrastructure for emergencies/business continuity purposes; and
- Maintain the CSP environment in accordance with the DoD Risk Management Framework (RMF).

The contractor shall provide the Government with cybersecurity materials, e.g. system security scans, configurations, proof of certification for system administrators, Federal Information Security Modernization Act of 2014, and DoD cybersecurity compliance information and artifacts as required under RMF within five business days of written request from the Government. The information shall be included in the Cloud Migration Report (Section F, Deliverable 21).

C.5.26 TASK 26 – TRANSITION OUT

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a draft Transition-Out Plan within 90 calendar days of Project Start (PS) (Section F, Deliverable 36). The Government will work with the contractor to finalize the Transition-Out Plan (Section F, Deliverable 37) in accordance with Section E. At a minimum, this Transition-Out Plan shall be reviewed and updated on an annual basis (Section F, Deliverable 38). Additionally, the Transition-Out Plan shall be reviewed and updated quarterly during the final Option Period (Section F, Deliverable 38).

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes.
b. Points of contact.
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel.
g. Schedules and milestones.
h. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

The TPOC will notify the contractor of all outstanding requirements that shall be completed prior to task order expiration which would include--

The contractor shall:

1. Ensure that all information assets and related configuration information are up to date and available for the Government's review at least five months prior to the expiration of the task order; and

2. Commence transition-out upon the execution of the transition-out optional CLIN or 120 calendar days prior to the end of the fourth Optional Period.

Phase 1: Ninety calendar days prior to the expiration of the task order, the incumbent contractor shall deliver to the Government images/VMs of the SMMS/RCMS-G development and test environments (development and test servers and workstations) with all associated tools, documents to include previous and source code:

1. Production: Images/VMs hosted at incumbent contractor site, related to current SMMS/RCMS-G production environment and solution files, team foundation server or any source code related to the application or sub-Applications;

2. Development: Images/VMs hosted at incumbent contractor site, used to develop SMMS/RCMS-G environment to include all production release version and solution files, team foundation server or any source code related to the application or sub-Applications;

3. Turn over all administrative access information, i.e., user-name and password to the ARNG at least 60 calendar days prior to the end of the contract;

4. Work with the incoming contractor in transitioning the operational support; and

5. Provide documentation and information as requested by the Government (the contractor shall deliver a copy of all current and relevant system documentation created during the contract).

Phase 2: The Government intends the following validation process:

1. Incumbent contractor work with the incoming contractor and necessary third parties to install the images of the system on development and test environments in a sandbox environment specified by the government.

2. The government will monitor the process of building the mirror system on the new environment to validate build guides and installation processes. The incumbent contractor will perform unit, system, and integration tests to ensure all modules are in working order.

3. The incumbent contractor shall conduct acceptance testing by comparing the output of the mirror system's applications against the production system results. The process will be observed by Government, incoming contractor, and third-party resources as necessary.

4. The transfer to the incoming contractor is not considered complete if the validation process is unsuccessful.

Phase 3: The contractor in accordance with its phase-out plan shall develop and execute an approach to transition program knowledge to the government and incoming contractor. This approach includes but is not limited to SOPs, plans, information papers, and lessons learned. Knowledge transferred shall include backup and restoration procedures.

C.5.27 SECTION 508 COMPLIANCE

Section 508 of the Rehabilitation Act requires Federal agencies to make their electronic and information technology (IT) accessible to people with disabilities. This applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology.

All electronic and information technology (EIT) procured through this task order must meet the applicable accessibility standards specified in 36CFR1194.2, unless an agency exception to this requirement exists. Any agency exceptions applicable to this task order are listed below.
The standards define Electronic and Information Technology, in part, as "any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. The standards define the type of technology covered and set forth provisions that establish a minimum level of accessibility. The application section of the standards (1194.2) outlines the scope and coverage of the standards. The standards cover the full range of electronic and information technologies in the Federal sector, including those used for communication, duplication, computing, storage, presentation, control, transport, and production. This includes computers, software, networks, peripherals, and other types of electronic office equipment.

Applicable Standards, which apply to this acquisition

Section 1194.21: Software Applications and Operating Systems ____X______.
Section 1194.22: Web-based Internet Information and Applications ____X_____.
Section 1194.23: Telecommunications Products _______________.
Section 1194.25: Self-Contained, Closed Products _____________.
Section 1194.26: Desktop and Portable Computers _____________.
Section 1194.31: Functional Performance Criteria ______________.